KOOWEERUP REGIONAL HEALTH SERVICE POLICY AND PROCEDURE MANUAL

Privacy/Confidentiality of Use of Patient/Resident Information

DOCUMENT TYPE

PROCEDURE

PURPOSE

Kooweerup Regional Health Service (KRHS) is committed to protecting the privacy of health information in accordance with the Health Records Act 2001 and other relevant legislation relating to privacy and confidentiality.

The purpose of this policy outlines the minimum obligations when handling health information, to meet our legal obligations and to protect it from improper use, disclosure, unlawful destruction or loss.

TARGET AUDIENCE

All persons including staff, contractors, agency staff, external organisations, students, vendors and volunteers, across all services within KRHS.

DEFINITIONS

- Personal information – personal information collected to provide or used in providing a health service is classified as health information and applies to this policy.

- Privacy breach – conduct constituting a breach of privacy includes, but is not limited to:

    - Accessing, using or directly/indirectly disclosing information for which there is no authorised or justifiable reason to fulfil the functions of your role (and to the extent necessary only).
    - Knowingly disclosing information about KRHS's activities to the media, contractor, tenderer or other party without proper cause or authority.
    - Behaviour or conduct that contradicts this policy, a related policy providers, guidelines or relevant legislation and places health information at risk of exposure to loss or access by unauthorised persons.

POLICIES

This policy applies to all health information collected, handled, used or stored across all services within KRHS, regardless of its method of capture including electronic, digitised, verbal, telephonic and paper-based information.

KRHS respects our customer's right to privacy. All persons with access to health information must take reasonable measures to ensure privacy and security of the information it holds. All persons with access to health information are subject to investigation, disciplinary action, dismissal or possible legal consequences if privacy is placed at risk or a breach occurs.

All persons who have access to health information must at all times:

- Maintain privacy and confidentiality as required by law.
- Sign Confidentiality Agreements as part of their engagement with KRHS.
    - Where external providers have access to information, their organisations overarching Service Contractor or Privacy Agreement may be accepted in place of a KRHS Confidentiality Agreement as agreed by the Chief Executive Officer or delegate.
- Ensure they are aware of and maintain, their obligations relating to privacy.
- Comply with related policies, providers and guidelines on the use, disclosure and security of information.
- Collect information only to the extent necessary to fulfil our obligations as a Health Service, by lawful and fair means only.
- Ensure individuals who they collect information about, are informed on our information handling practices.
- Act in accordance with Professional Codes of Conduct and Ethics; and
- Rise any identified privacy concerns and report any potential privacy risks or breaches to the KRHS Chief Executive Officer.

See Appendix for a summary of Health Privacy Principles.

NOTE:

For the purposes of this Policy, information includes verbal, written, computerised, filmed/photographic records and registers of any kind.

ACTION TO BE TAKEN WHEN A BREACH OF CONFIDENTIALITY/PRIVACY IS IDENTIFIED:

Complete an Incident Report stating who was involved, what information was involved, why it occurred, when it occurred and what action has been taken.

Decided what action is to be taken.

Review education and training in Confidentiality with the person(s) involved.

Take appropriate disciplinary action against the person(s) involved. (Note: that a significant wilful breach of confidentiality can potentially be found to be gross and wilful misconduct and lead to the termination of the staff member involved).

Discuss the matter with your Supervisor.

Complaint Handling under the Privacy and Data Protection Act 2014 (No. 60 of 2014):

- Refer to KRHS Reporting Privacy Breaches Policy.

- Complaint received by of the Office of the Privacy and Data Protection Commissioner (must relate to personal information held before 1 September 2002).

- Complaint identified as being relevant, if relevant respondent organisation notified as soon as practicable, details of complaint given.

- Commissioner has 90 days to decide to act on complaint and seek information before making decision.

- If complaint declined, the complainant may within 60 days require the Commissioner to refer matter to Victorian Civil and Administrative Tribunal (V.C.A.T.).

- Commissioner has obligation to try and conciliate complaints. The Commissioner can require a party to attend a Conciliation.

- The Commissioner can decide Conciliation is not reasonably possible – if tried but fails both parties must be notified in writing. The complainant can within 60 days have the complaint referred to V.C.A.T.

If V.C.A.T. finds any part of a complaint proven it can:

- Order prohibiting the organisation from repeating/continuing conduct that interferes with complainant's privacy.

- Order the organisation redress the loss/damage suffered by complainant or

- Order the organisation pay compensation of up to $100,000 to complainant.

NOTE: Complaints Forms are available from S. Gregory in Administration.

EVALUATION

Privacy breach investigations, regular document revision and review of relevant 'Riskman' Reports will be used to evaluate the effectiveness of this policy.

DESIRED OUTCOME

Information that is held in relation to patients/residents/clients/staff is utilised according to the relevant Acts, Regulations and Principles.

KEY LEGISLATION, ACTS AND STANDARDS

- Health Records Act 2001 (VIC). Version No. 031. Version incorporating amendments as at 1 July 2016. Retrieved August 17, 2016 from http://www.austlii.edu.au/au/legis/vic/consol_act/hra2001144/
- Mental Health Act 2014 (No. 26 of 2014). (VIC). Retrieved August 2016 from http://www.austlii.edu.au/au/legis/vic/num_act/mha201426o2014174/
- National Safety and Quality Health Service Standards (2012, September). Retrieved May 19, 2016 from http://www.safetyandquality.gov.au/wp-content/uploads/2011/09/NSQHS-Standards-Sept-2012.pdf
- Privacy Act 1988. (Cwlth). No. 73. Registered 18 July 2016. Retrieved August 17, 2016 from http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/
- Health Services Act. (VIC). Versional No. 151. Version incorporating amendments as at 1 July 2016. Retrieved August 17, 2016 from http://www.austlii.edu.au/au/legis/vic/consol_act/hsa1988161/
- Freedom of Information Act 1982. (VIC). Version No. 090. Version incorporating amendments as at 17 March 2016. Retrieved August 17, 2016 from http://www.austlii.edu.au/aulegis/vic/consol_act/foia1982222/

RELEVANT STANDARDS:

<#accreditation_tags>

APPENDIX
SUMMARY OF HEALTH PRIVACY PRINCIPLES

The Health Records Act contains eleven Health Privacy Principles that outline how much information must be handled.

HEALTH RECORDS ACT 11 HEALTH PRIVACY PRINCIPLES (HPPs)	
HPP1	Collection
HPP2	Use and Disclosure
HPP3	Data Quality
HPP4	Date Security and Data Retention
HPP5	Openness
HPP6	Access and Correction
HPP7	Identifiers
HPP8	Anonymity
HPP9	Transborder Data Flows
HPP10	Transfer of closure of the practice of a health service provider
HPP11	Making information available to another health service provider

The summary below is not intended to detail all of the legislative requirements. A copy of the Acts is available using the hyperlinks within this policy.

HPP1 Collection

KRHS is permitted to collect information necessary to fulfil its functions as a service provider or where required by law. Information must only be collected by fair and lawful means and where possible directly from the individual themselves.

KRHS must inform consumers on the organisations information handling practices and their rights, which is done through print media at various entry points across KRHS, the KRHS Website or verbal explanation as requested.

HPP2 Use and Disclosure

Information is only permitted to be used or disclosed for the primary purpose for which it was collected or a directly related secondary purpose. Information may be used or disclosed for other purposes, with the individuals consent or as permitted or required by law.

De-identified – information that is de-identified and the identity of the person cannot reasonably be ascertained, can be sued without consent. Considerations should be given when de-identifying information, as removing

a name or date of birth may not be sufficient depending on the information being used.

HPP3 Data Quality

KRHS and all individuals who have access to information, must take reasonable steps to ensure the information they capture, detail or hold is up-to-date, accurate, complete and relevant to KRHS functions.

HPP4 Data Security and Data Retention

KRHS must take reasonable steps to protect the health information its holds from misuse and loss and from unauthorised access, modification or disclosure.

KRHS is also not permitted to delete health information relating to an individual, even if it is later found or claimed to be inaccurate, unless required by law. To meet these requirements information must be securely retained in accordance with related retention schedules. Health information must not be destroyed unless approved by KRHS Chief Executive Officer.

HPP5 Openness

KRHS must have clearly expressed policies on its management of health information and the steps that an individual must take in order to obtain access to their health information, which are available in PROMPT.

Where this is a privacy breach, KRHS must notify the affected individual as well as the Health Services Commissioner of the incident.

HPP6 Access and Correction

Under the Freedom of Information Act 1982, consumers have the right to request access to their health information. In some circumstances access may be refused, in these circumstances an explanation will be provided.

Under the Freedom of Information Act 1982, consumers also have the right to request an amendment to their health information.

KRHS must comply with these obligations and have processes in place to meet this legislative requirement.

HPP7 Identifiers

KRHS may only assign identifiers to consumers if the assignment of identifiers is reasonably necessary to carry out any of its functions efficiently.

For the purpose of accurate and timely identification, a Unique Record (UR) Number must be allocated to each consumer that attends KRHS.

To participate in national eHealth strategies, KRHS is required to use healthcare identifiers to secure transmit information to consumers My Health Record. This will include the use of Individual Healthcare Identifier (IHI), Healthcare Provider Identifier – Individual (HPI-I) and Healthcare Provider Identifier – Organisation (HPI-O).

HPP8 Anonymity

Wherever it is lawful and practicable, KRHS must provide consumers with the option of not identifying themselves when entering its health service.

Identification is required for KRHS to provide safe and quality care to our consumers and to comply with relevant legislation (i.e. reportable disease or notifiable events). Thus, to meet this requirement, when requested, KRHS must provide a consumer with an alias name under their allocated UR number.

HPP9 Transborder Data Flows

KRHS is not permitted to transfer information outside Victoria, unless:

- They reasonably believe the recipient of the information will uphold fair handling of the information under substantially similar privacy principles.
- The transfer is required by law.
- It is necessary to less or prevent a serious or imminent risk to the life, safety or wellbeing of an individual, or
- Where consent has been obtained from the individual.

HPP10 Transfer or closure of the practice of a health service provider

KRHS must act in accordance with this principle in the event KRHS or part thereof is sold, transferred, amalgamated or closed down.

HPP11 Making information available to another Health Service Provider

KRHS must make information available to another health service provider, as soon as practicable, upon request of the individual or authorised health service provider as detailed under HPP2 Use and Disclosure.